

Kaspersky Internet Security 2011

KIS 2011 使用手冊

版本：1.1

發佈時間：2010 / 07 / 13



硬體和軟體需求

為了確保應用程式的各項功能正常運作，需符合以下最低的軟/硬體需求：

- *一般需求：*
  - 480 MB 硬碟空間
  - 光碟機（用以從光碟安裝應用程式）
  - Microsoft Internet Explorer 6.0 或以上（用以透過網路更新應用程式資料庫和模組）
  - Microsoft Windows Installer 2.0 或以上
  - 電腦滑鼠
  - 網際網路連線（用以啟動產品）

- *系統需求：*
  - *Windows XP Home Edition（SP2 以上）、Windows XP Professional （SP2 以上）、Windows XP Professional x64 Edition（SP2 以上）：*
    - Pentium 800 MHz 以上（或同等級處理器）
    - 512 MB 記憶體

＊沙盒防護無法使用於 *Windows XP* 64 位元作業系統。

  - *Windows Vista Home Basic(32/64 位元)、Windows Vista Home Premium（32/64 位元）、Windows Vista Business（32/64 位元）、Windows Vista Enterprise（32/64 位元）、Windows Vista Ultimate（32/64 位元）：*
    - Pentium 1 GHz 以上（或同等級處理器）
    - 1 GB 記憶體 *(32 位元)*; 2GB 記憶體 *(64 位元)*
  - *Windows 7 Starter（32/64 位元）、Windows 7 Basic（32/64 位元）、Windows 7 Home Premium(32/64 位元)、Windows 7 Professional(32/64 位元)、Windows 7 Ultimate（32/64 位元）：*
    - Pentium 1 GHz 以上（或同等級處理器）
    - 1 GB 記憶體 *(32 位元)*; 2GB 記憶體 *(64 位元)*

＊ 安裝於 *Windows 7* 64 位元、*Windows Vista* 64 位元作業系統時，沙盒防護部分功能會受到限制。

- *小筆電系統需求：*
  - Intel Atom 1.33 MHz（Z520）以上（或同等級處理器）
  - Intel GMA950 64 MB 以上記憶體顯示卡
  - 螢幕視窗必須大於 10.1 吋
  - *Windows XP Home Edition（SP2）或以上作業系統*

功能升級及新增特性

- 全新的系統監控防護元件：監控系統中所監控的應用程式活動資訊可提供其他防護功能判斷分析。當防護元件偵測到可疑程式執行動作後可根據應用程式活動記錄，將可疑程式所執行的動作進行回溯。
- 沙盒防護功能更進化：使用沙盒防護於獨立的環境執行可疑應用程式，完全不需擔心影響作業系統。
- 加入提升網路安全性的新功能：
  - 安全瀏覽 – 包括 KIS 2010 中的網址連結掃瞄功能之外，還能封鎖存取惡意網站，讓您安心地遨遊網際網路。
  - 區域篩選 – 讓您根據網站所屬的網域決定允許或拒絕開啟網站。藉由此功能，您可以封鎖屬於高感染風險區域內的網站。
- 應用程式控制：提供更有效的應用程式狀態分析，還使用長期統計而成的 KSN 資料庫規則加以判斷，確保程式安全無虞。
- 藉由背景掃瞄模組：可以讓電腦於閒置時進行病毒掃瞄，而當您回來使用電腦時自動停止掃瞄。在您使用電腦時保持運作效能，同時可以兼顧電腦的安全性。
- 家長控制功能增強：您可以使用家長控制來限制用戶使用電腦或網路及應用程式，限制存取含有不當內容的網站或是任何下載行為。不僅控制用戶於社交網路或即時通訊的互動行為，並可檢視用戶行為報告。為了方便管理家長控制設定，您可以儲存或載入每個用戶的設定內容。

電腦防護的基本概念

Kaspersky Internet Security 防護已知與未知的威脅、網路與入侵攻擊、垃圾郵件與其它不必要的資訊干擾您的電腦。每一種威脅都由各自的防護元件進行處理。各個元件都能加以設定及獨立關閉或啟用。

除了防護元件持續提供的保護之外，我們建議您定期的執行完整掃瞄。這是相輔相成的方式來避免防護元件尚未偵測的惡意程式繼續存在。因為某些原因，當您可以元件防護等級或關閉某些防護時，就可以藉由掃瞄協助您完整防護電腦。

為了使 Kaspersky Internet Security 保持在最新的狀態，您必須定期更新資料庫及升級程式版本。預設將會自動進行資料庫更新。但必要時，您仍可以隨時點選更新及手動升級程式版本。

您可以使用應用程式控制個別管理電腦上所開啟的應用程式。應用程式控制是根據程式資訊內容進行管理，這些程式資訊通常是包含設定及重要資料的檔案、資料夾或登錄機碼，及使用者檔案（我的文件資料夾、Cookies 及使用者活動歷程等）。當您發現應用程式有安全性疑慮時，可以使用沙盒防護開啟程式。

某些需要偶爾使用的特定工作可以使用內建的工具或精靈來執行，例如瀏覽器設定或隱私清理精靈。

Kaspersky Internet Security 防護元件

我的防護中包括三個群組，由不同程式元件進行防護：

- 檔案文件、個人數位身分資料、使用者帳號及密碼和信用卡資訊等，由檔案防護、應用程式控制及免疫防護提供防護。
- 電腦中所安裝的應用程式或作業系統檔案，由郵件防護、網頁防護、即時通訊防護、應用程式控制、系統監控、免疫防護、網路攻擊防護及垃圾郵件防護提供防護。
- 線上安全包含網路銀行、線上購物電子付費系統或垃圾及病毒電子郵件等，由郵件防護、網頁防護、即時通訊防護、駭客防護、網路攻擊防護、垃圾郵件防護、網路釣魚防護、廣告橫幅防護及網路監控提供防護。

您可以在應用程式主控台中點選**我的防護**，於右方的圖表詳細檢視各個群組所使用的防護元件。

防護元件即時提供電腦全面性的防護：

檔案防護

檔案防護可以預防電腦中的檔案受到感染。當系統啟動時檔案防護將會掃瞄您開啟、儲存或執行的檔案以及所有連接的磁碟。Kaspersky Internet Security 會攔截每次存取檔案的動作並掃瞄檔案是否安全。確認檔案為受感染或正常之後才能開啟使用。如果檔案受感染且無法解毒，將會立即刪除並建立備份或直接將檔案移至隔離區。

郵件防護

郵件防護可以掃瞄經由傳送及接收郵件中的惡意檔案。如果於郵件中偵測到威脅，防護元件將執行相關的處理動作；若未發現威脅，郵件將立即恢復使用。

網頁防護

網頁防護能攔截或封鎖網頁中具有威脅的惡意指令碼，也將會監控所有 HTTP 流量。此外還能封鎖惡意網站的存取。

即時通訊防護

即時通訊防護藉由掃瞄即時通訊軟體協議所接收的資訊，確保使用即時通訊軟體時的安全性。讓您絕對安心地使用任何一款即時通訊軟體。

應用程式控制

應用程式控制記錄電腦中的應用程式執行狀況，並根據群組中訂定的規則管理程式活動。每個應用程式群組都有預設的規則，用來判斷程式是否有存取電腦資源的權限。

系統監控

監控系統中所監控的應用程式活動資訊，可提供其他防護功能判斷分析使用。如果開啟儲存活動記錄的功能，當電腦產生任何異常時，您可以執行回溯可疑程式動作恢復遭惡意程式變更的設定。

駭客防護

駭客防護確保區域網路與網際網路的使用安全。防護元件使用兩種不同類型的規則：應用程式規則與封包規則，過濾所有的網路活動。

免疫防護

免疫防護提供主動防禦技術，在最新的惡意程式威脅危害系統前即可偵測處理。免疫防護將監控及分析電腦所有應用程式程式的行為。Kaspersky Internet Security 根據這些行為來判斷是否具有危險性。所以除了防範已知威脅外，也能偵測還沒有被發現的未知威脅。

網路攻擊防護

網路攻擊防護會在作業系統啟動時自行載入，追蹤網路流量是否含有網路攻擊的行為特徵。一旦在電腦上偵測到網路攻擊，Kaspersky Internet Security 會封鎖進行攻擊的電腦，中止攻擊行為。

垃圾郵件防護

垃圾郵件防護將整合於您所安裝的郵件收發軟體，並檢查過濾接收的所有垃圾郵件。含有垃圾內容的郵件會被標示特殊的主旨。防護元件提供過濾選項，您可自行定義要刪除或是將垃圾郵件移至指定資料夾。垃圾郵件防護也會掃瞄郵件中是否包含網路釣魚網址。

廣告橫幅防護

廣告橫幅防護封鎖應用程式或瀏覽器介面中所顯示的廣告資訊。

網路監控

網路監控元件可以即時檢視網路活動及流量的所有資訊。

網路釣魚防護

與網頁防護、垃圾郵件防護和即時通訊防護整合的防護元件，用來過濾網址是否位於網路釣魚或可疑網址資料庫。

家長控制

家長控制元件用來防止幼童或青少年使用電腦或上網時，接觸到不良資訊。您可以根據不同年齡層彈性地設定存取網路或應用程式的限制條件。當然您也可以檢視這些使用者的統計報告。

安裝

利用設定精靈來安裝 KIS 2011。

建議在安裝前，先關閉所有執行中的應用程式。

要在您的電腦安裝 KIS 2011，請執行產品光碟中的安裝程式（*.EXE 檔）。

透過網路下載的安裝程式與光碟片裡面的程式是相同。
建議您在安裝前，先至卡巴斯基網站檢查是否有新版的應用程式。

卡巴斯基安裝程式在開始安裝時，將會透過網際網路搜尋卡巴斯基實驗室伺服器上是否有新版的安裝程式，當有搜尋到新版的安裝程式，便會提示您進行下載，當下載完畢，即立刻開始安裝，若取消下載，安裝程式將繼續原有的安裝步驟。

應用程式安裝是透過精靈來完成，每個視窗包含一組按鈕以控制安裝程序，以下將說明它們的作用：

- **下一步** ：同意動作，並切換到下一個安裝程序。
- **上一步** ：返回上一個安裝程序。
- **取消**：取消安裝。
- **完成**：完成應用程式安裝過程。

詳細的安裝步驟將在以下介紹。

步驟 1、搜尋是否有新版的應用程式

若是透過光碟進行安裝，或已經下載安裝程式一段時間，建議您在安裝前先至卡巴斯基官方網站（www.kaspersky.com.tw）檢查是否有新版本的應用程式。

產品下載連結：
http://www.8066.com.tw

注意：建議您安裝最新版的應用程式，以獲得最佳的相容性與效能。

步驟 2、確認您的系統符合安裝需求

安裝前請先確認電腦的作業系統和更新程式（service packs）符合「硬體和軟體需求」，並請確認您擁有安裝軟體所需的管理者權限。

若未符合需求，螢幕上會顯示相關的通知訊息。我們建議您在安裝卡巴斯基實驗室的產品之前，先透過 **Windows Update** 服務安裝更新程式。



步驟 3、選擇安裝類型

如果您的系統已符合需求，且在卡巴斯基實驗室上沒有新的版本，或者您已經取消較新版本的安裝，設定精靈將會安裝目前的版本至您的電腦中。

在此安裝步驟，您可以選擇最適合您的安裝項目：

- **快速安裝**：請點選**下一步**直接進行安裝（□**自訂安裝**項目未選取），應用程式將會依照卡巴斯基實驗室的建議安裝應用程式。在安裝完成之後，應用程式設定精靈將會啟動。
- **自訂安裝**：在這個情況之下（☑**自訂安裝**項目已選取），您可以指定應用程式的安裝路徑，且可透過精靈啟動與設定應用程式。

如果您選擇第一項（快速安裝），應用程式設定精靈將會要求您檢視授權協議書與 Kaspersky Security Network 資料收集聲明。接下來，應用程式將會安裝至您的電腦中。

如果您選擇第二項（自訂安裝），將會在每一個安裝步驟被要求進行確認。要進行安裝，請點選**下一步**。取消安裝，請點選**取消**。

步驟 4、檢視授權協議書

在此步驟，您應該檢視與卡巴斯基實驗室之間的授權協議書。

- 請仔細閱讀協議書，如果您同意協議內容，請點選**接受**按鈕。應用程式將繼續。
- 取消安裝，請點選**取消**按鈕。

步驟 5、Kaspersky Security Network 資料收集聲明

在此步驟，您將參與 Kaspersky Security Network 計畫。傳送在您電腦中偵測到的新威脅至卡巴斯基實驗室，傳送由卡巴斯基實驗室分配的唯一 ID 號碼與系統資訊。在此，卡巴斯基實驗室保證隱私資料將不會被洩漏。

請檢視 Kaspersky Security Network 資料收集聲明。如果您同意所有的協議，請保留勾選 V **我同意參與 Kaspersky Security Network**，然後點選**安裝**按鈕。

步驟 6、搜尋其他不相容的軟體

在此步驟，精靈將搜尋其他廠牌的防毒軟體或不相容的程式，因為這些程式會與 Kaspersky Internet Security 產生衝突。如果沒有發現任何不相容的軟體，精靈將會自動進行下一個安裝步驟。

如果在您的電腦中發現其他的防毒軟體，將會顯示於螢幕。在您安裝之前會要求進行移除。移除完畢後請務必重新啟動電腦。

之後精靈將會繼續進行安裝，請點選**下一步**按鈕。

步驟 7、選擇目的地資料夾

只有選擇自訂安裝才會出現此步驟。

在這個步驟，您將確認要安裝應用程式的資料夾。預設路徑為：

- <disk>\Program Files\Kaspersky Lab\Kaspersky Internet Security 2011\ - 32 位元作業系統
- <disk>\Program Files（x86）\Kaspersky Lab\Kaspersky Internet Security 2011\ - 64 位元作業系統

您也可以指定其他的資料夾，請點選**瀏覽**按鈕，在標準資料夾視窗中選擇資料夾，或輸入欲安裝的路徑。

請記住！如果您是以手動的方式輸入完整安裝路徑，最多不可以超過200個字元或包含任何特殊字元。

設定完成，請點選**下一步**按鈕。

步驟 8、準備安裝

只有選擇自訂安裝才會出現此步驟。完整安裝將會略過此步驟。

在初始化與自訂安裝應用程式時，建議您勾選**在安裝前啟用自我防護功能**。若在安裝過程中發生錯誤，此功能可協助您回溯至原本的狀態。若無法正常安裝完成，嘗試再次安裝時，則建議您取消勾選此項目。

如果透過 Windows 遠端桌面的方式安裝，建議取消勾選**在安裝前啟用自我防護功能**，如果勾選此項，安裝程序可能會中斷或安裝異常。

如果您使用遠端桌面方式安裝，且尚未取消勾選此功能，請按**取消**跳出設定精靈。重新進行安裝後點選**自訂安裝**並取消勾選**在安裝前啟用自我防護功能**即可繼續安裝。

設定完成，請點選**安裝**按鈕。

當在 Windows XP 安裝 Kaspersky Internet Security 元件時，目前的網路連線將被終止。被終止的連線將在稍後恢復。

步驟 9、開始安裝

安裝應用程式元件將會需要一點時間，請稍後精靈完成安裝。一旦所有元件安裝完畢，精靈將會自動進行到下一個步驟。

- 如果安裝過程因為有病毒或惡意程式導致錯誤，企圖讓安裝程序失敗，設定精靈將會顯示解毒工具下載訊息。
- 如果您要下載解毒工具，設定精靈將會自動從卡巴斯基實驗室伺服器下載，並在下載完成後立即執行安裝。如果遇到無法下載時，請您自行點選或輸入網址前往下載。
- 當您執行完解毒工具並刪除病毒後，請重新執行安裝步驟。

步驟 10、啟動應用程式

您必須完成啟動程序後才能使用完整功能。

您必須連線網際網路才能進行啟動程序。

啟動方式總共有三種：

- **啟動商業授權**：以註冊後所取得的「啟動碼」來進行啟動。

如果您輸入 Kaspersky Anti-Virus 啟動碼，安裝程序將會在啟動程序完成後自動切換為安裝 Kaspersky Anti-Virus。

- **啟動試用授權**：安裝試用版本，並試用完整功能一個月（一台電腦僅能試用一次），試用期結束後將無法繼續啟動試用授權。
- **稍後啟動**：第一次安裝啟動時可選擇稍後啟動，但選擇該選項後僅能進行一次病毒資料庫更新。

如果 Kaspersky Internet Security 安裝完成後隨即被移除，授權資訊仍會被儲存。

繼續進行安裝，請點選**下一步**按鈕。

步驟 11、完成啟動程序

安裝精靈將會顯示啟動程序完成訊息，告知您已經成功安裝授權，並會顯示授權的相關資訊：授權類型（試用或商業授權）、授權使用的電腦數量及授權到期日。

繼續進行安裝，請點選**下一步**按鈕。

步驟 12、系統分析

本步驟將會針對 Microsoft Windows 作業系統所包含的應用程式建立信任清單，以防止系統檔案執行時遭受限制或進行多餘的掃瞄。

當分析完畢後，設定精靈將會自動下一個步驟。

步驟 13、安裝完成

設定精靈完成所有步驟後將會顯示安裝完成。要開始使用 Kaspersky Internet Security，請確認已經勾選**啟用 Kaspersky Internet Security**，並點選**完成**。

某些狀況下，您會需要重新啟動電腦才能完成安裝。

如果已經勾選**啟用 Kaspersky Internet Security**，將會於重新啟動電腦後自動執行 Kaspersky Internet Security。

如果取消勾選**啟用 Kaspersky Internet Security**，之後您必須自行手動開啟 Kaspersky Internet Security。

開始使用

Kaspersky Internet Security 完成安裝後就可以立即使用。為了確保防護功能確實運作，建議您完成安裝設定後馬上依照下列步驟操作：

- 更新資料庫。
- 執行**完整掃瞄**及**弱點掃瞄**。
- 確認電腦防護狀態為受到防護，如果電腦存在安全性風險，請點選**立即修復!**來解決。

更新應用程式

注意！您必須連上網際網路才能更新 Kaspersky Internet Security。

Kaspersky Internet Security 的資料庫包含威脅特徵碼、垃圾郵件的詞組、網路攻擊的說明…等。然而，當應用程式安裝後，其所包含的資料庫會變成過期，因為卡巴斯基實驗室會定期更新資料庫和應用程式模組。

您可以在應用程式設定時，選擇合適的更新模式。預設下，KIS 會自動檢查卡巴斯基伺服器的更新，若伺服器上有新的更新，KIS 就會下載並安裝。

為了保持您的電腦在最新的防護狀態下，我們建議您在安裝後**立即更新**。

手動更新 Kaspersky Internet Security：

1. 開啟主控台。
2. 點選左邊視窗的**更新中心**。
3. 點選**開始更新**。

掃瞄電腦病毒

惡意軟體的作者一直努力掩飾他們的執行程序，因此，您也許不會注意到電腦上存在著惡意軟體。

當應用程式安裝後，它會自動執行**即時掃瞄**。這個工作能夠搜尋和清除在系統啟動時所載入的惡意檔案。我們同時建議您定期執行完整掃瞄工作。

開始/停止病毒掃瞄工作：

1. 開啟主控台。
2. 在左邊視窗選擇**我的掃瞄**（完整掃瞄、快速掃瞄）。
3. 點選**開始完整掃瞄/開始快速掃瞄**就會進行掃瞄工作。

掃瞄電腦弱點

您的電腦可能由於所安裝的應用程式包含漏洞，導致系統遭到入侵而被破壞。為了找出問題並加以排除，建議您使用弱點掃瞄功能。

開始弱點掃瞄工作：

1. 開啟主控台。
2. 在左邊視窗選擇**安全工具箱**。
3. 選擇**弱點掃瞄**。
4. 點選**開始**。

管理授權

卡巴斯基需要利用合法的商業授權進行線上啟動才能使用完整操作。授權檔案內含授權編號、授權類型、啟動日期及授權到期日等相關資訊。

第一次安裝 KIS 過程中，如果您沒有啟動商業授權或試用授權，選擇**稍後啟動**，那麼 KIS 將只會進行一次更新病毒資料庫，而不會更新本身的程式版本。若您是使用試用版本，一旦試用到期後更新功能將會停止運作。

當商業授權到期後，卡巴斯基仍可繼續運作，但更新功能將被停用。您仍可使用其他的防護元件及利用到期前的資料庫來進行掃瞄。為了使電腦受到完善的保護，授權到期前兩週將會在卡巴斯基啟用時提醒您授權即將到期。建議您在到期前立刻更新授權。

- 檢視授權協議請點選**檢視終端使用者授權協議**。
- 刪除授權請點選授權編號旁邊的 **X** 圖示。
- 啟動新的商業授權請點選**啟動商業授權**。
- 需要更新或購買授權請點選**購買授權**連線到相關網頁進行購買。

移除 Kaspersky Internet Security

移除Kaspersky Internet Security後，您的電腦及個人資料將無法受到保護。

卡巴斯基設定精靈將協助您移除 Kaspersky Internet Security，啟動精靈方式如下：

點選**開始**後進入**程式集**，點選 Kaspersky Internet Security 2011 內的**修復或移除**，於接下來開啟的頁面中點選**移除**。

步驟 1、儲存物件

此步驟您可以選擇儲存於下次安裝時使用的相關資訊。例如當新版本推出時，您可以儲存目前資訊以利後續安裝時直接套用。

預設將會完整解除安裝，全部資料將不保留。

•儲存應用程式物件的方式如下：

1. 選擇**儲存應用程式物件**。
2. 勾選您要儲存的項目類型：
   - **啟動資料** – 若授權尚未到期，在下次安裝時可以自動套用此啟動資料。
   - **垃圾郵件防護資料庫** – 包含目前所使用的垃圾郵件特徵碼。
   - **備份及隔離區資料庫** – 經掃瞄後放置於備份及隔離區的檔案。
   - **防護設定** – 包含目前使用的功能設定。
   - **iSwift 和 iChecker 資料** – 執行過掃瞄後的資訊檔案。
   - **沙盒防護資料夾的資料** – 使用沙盒防護所儲存於沙盒防護資料夾的檔案。

步驟 2、確認執行移除

一旦移除所有元件之後，您的電腦及個人資料將不再受到保護，此頁面將會請您再次確認是否移除所有應用程式元件。確認要解除安裝，請按**移除**。

移除過程中要停止移除動作，您可以隨時點選**取消**中止移除安裝的操作。

步驟 3、開始執行移除

此步驟設定精靈將會移除電腦上所安裝卡巴斯基應用程式元件。請稍後，解除安裝步驟完成。

當您完成解除安裝後必須重新啟動電腦。如果您沒有立即重新啟動電腦，移除程序將會先暫停，直到您稍後重新啟動電腦才會完成整個移除步驟。

應用程式操作介面

應用程式具備友善、簡單、易用的操作介面。

除了主程式介面，還有一些外掛程式，包含 Microsoft Office Outlook、Microsoft Outlook Express（Windows Mail）、The Bat!（掃瞄病毒和垃圾郵件）、Thunderbird、Thunderbird、Mozilla Firefox、Microsoft Internet Explorer 和 Microsoft Windows Explorer。上述的外掛程式可以延伸主程式功能，管理和調整相關防護元件。

通知區域圖示

安裝應用程式後，卡巴斯基圖示會顯示在 Microsoft Windows 工作列的通知區域。

這個圖示是應用程式運作的指標，它能反應出防護狀態和正在執行的工作。如果是鮮明的彩色圖示，表示所有或部份防護元件正在執行；假如是灰色圖示，表示所有的防護元件已停用。

應用程式圖示會依照執行的工作而改變狀態：

- －掃瞄電子郵件。
- －掃瞄網路流量。
- －更新應用程式資料庫和應用程式模組。
- －電腦需要重新啟動以套用更新。
- －某些元件發生錯誤或所有防護元件已停用。

要開啟快捷選單，請在圖示上按滑鼠右鍵。

若要開啟應用程式主控台，請在圖示上點擊滑鼠左鍵 2 下。

假如有啟用新聞通知，當卡巴斯基實驗室的新聞送達時，新聞圖示會出現在通知區域。以滑鼠點擊即可檢視新聞。

快捷選單

在此選單，您可以執行基本的防護工作。

此選單包含下列項目：

- **更新**：開始應用程式模組和資料庫更新，並安裝更新至電腦。
- **工具**：可開啟下列功能或設定-
  - **應用程式控制**：開啟應用程式活動視窗。
  - **網路監控**：開啟網路監控視窗。檢視網路連線、連接埠和流量的清單。
  - **虛擬鍵盤**：顯示虛擬鍵盤。
- **用沙盒執行應用程式**：開啟安全的應用程式執行環境，而不會有任何危險疑慮。點選後將會切換至沙盒防護模式。當執行沙盒防護時，您可以使用快捷選單內的**回到主控台**來切換回到正常桌面下操作。
- **Kaspersky Internet Security**：開啟應用程式主控台。
- **暫停防護/恢復防護**：暫時停用或啟用即時防護元件。這個選項並不會影響產品更新或病毒掃瞄工作的執行。
- **開啟家長防護/關閉家長防護**：開啟或關閉目前使用者家長控制功能。
- **設定**：開啟應用程式設定頁面。
- **關於**：顯示應用程式的相關資訊。
- **離開**：關閉應用程式（當選擇此項目之後，應用程式會從電腦記憶體中卸載）。

假如病毒掃瞄工作正在執行時，開啟快捷選單可看到工作狀態（完成百分比）。應用程式會依照您在快捷選單所選擇的工作，而移至相對應的主控台視窗。

應用程式主控台

主控台包含三個部份：

- 最上面的視窗，顯示電腦目前的防護狀態。總共有三種防護狀態，每一種狀態會顯示不同的顏色，就像紅綠燈的燈號一樣。
  - 綠色表示電腦處於正常的防護狀態。
  - 黃色和紅色表示有安全威脅，包含設定及應用程式操作、惡意軟體、資料庫過期、停用防護元件…等，這些安全威脅必須消除，請點選**立即修復!**來檢視詳細資訊與修復。

- 導航欄：用來快速切換到任意應用程式功能，執行病毒掃瞄工作及更新工作等。
- 右邊視窗包含應用程式的功能資訊，方便您調整各項設定、執行病毒掃瞄和下載更新等。

您也可以使用以下按鍵：

- **設定**：切換到應用程式設定。
- **報告**：切換到事件清單列表。
- **隔離區**：切換到已偵測威脅。
- **授權**：切換到授權管理。
- **我的卡巴斯基帳號**：可連線至技術支援網站建立個人帳戶。
- **支援**：開啟系統資訊和卡巴斯基實驗室的相關資源（技術支援服務、論壇）。
- **說明**：切換到應用程式說明。

注意：您可以變更應用程式的介面外觀，使用自訂的圖片和顏色。

通知

假如在應用程式運行時發生事件，Microsoft Windows 工作列上的卡巴斯基圖示就會跳出通知訊息。

依據事件對電腦安全的嚴重性程度，您可能會接收到下列數種通知：

- **警示**：當發生關鍵事件。舉例來說，當您的系統偵測到病毒或危險行為，應該立即決定要做出何種反應。這種類型的通知為紅色。
- **警告**：發生潛在危險事件。舉例來說，您的系統偵測到潛在感染檔案或可疑活動時，您必須告知應用程式該事件的危險程度。這種類型的通知為黃色。
- **通知**：並不緊急的事件。例如內容過濾元件的相關操作。這種類型的通知為綠色。

應用程式設定視窗

應用程式設定視窗可以從主控台或快捷選單來開啟。

要檢視這個視窗，請點選主控台右上角的**設定**，或選擇快捷選單中的設定。

各項元件、設定項目或其他內容都放置於左側上方的四種群組內。

- **防護中心**
- **我的掃瞄**
- **更新中心**
- **進階設定**

設定視窗包含兩部份：

- 左邊視窗可以存取應用程式元件、病毒掃瞄工作和更新工作等。
- 右邊視窗包含各元件及工作的設定。

Kaspersky 小工具

當 Kaspersky Internet Security 安裝於 Microsoft Windows Vista 或 Microsoft Windows 7 作業系統時，您可以使用 Kaspersky 小工具。

小工具可以讓您更快速開啟主要功能選項：防護狀態、病毒掃描和報告等。

當 Kaspersky Internet Security 安裝於 Microsoft Windows 7 時，小工具將會自動於桌面上顯示。當安裝於 Microsoft Windows Vista 時，必須由您手動將小工具新增至 Microsoft Windows 工具。

小工具的顏色直接表明目前電腦的防護狀態，如同主控台顯示的防護狀態。綠色表示電腦受到良好防護，黃色代表存在安全性風險，而紅色則代表電腦存在危險性風險。灰色則表示目前狀態是暫停防護。

小工具也會顯示更新狀態：當下載資料庫更新或模組更新時，小工具上會出現旋轉的地球圖示。

您可以使用小工具介面來執行下列主要工作：

- 檢視報告
- 開啟主控台
- 開啟沙盒防護

設定小工具

小工具的兩個快捷鍵可以由您自訂選項功能：

- 編輯設定
- 檢視報告
- 執行沙盒防護
- 檢視家長控制報告
- 檢視網路監控狀態
- 暫停/恢復防護

另外，您也可以變更小工具的顯示介面。

設定小工具的方式如下：

1. 將滑鼠游標移至小工具並開啟右方的選項。在左右邊圖示的下拉式選單選擇要顯示的功能。
2. 於上方的左右箭頭即可選擇小工具介面。
3. 完成後按**確定**。

暫停防護

當 Kaspersky Internet Security 安裝完畢後將會在每次系統開啟時自動執行。您可以手動選擇暫停即時防護，指的是暫時停止所有防護一段時間。

要暫停防護您的電腦：

1. 從**快捷選單**中，選擇**暫停防護**。
2. 暫停防護視窗會被開啟，請選擇您要啟用防護的時間：
   - **設定暫停防護時間<時間間隔>：**在指定的時間之後，防護將被啟用。請從下拉選單中選擇合適的時間間隔。
   - **重新開機後恢復防護：**防護將在系統重新啟動後恢復（需勾選**在電腦啟動時，啟動 Kaspersky Internet Security**）。
   - **暫停防護：**防護由您手動恢復。若要啟用防護，請從快捷選單中選擇**恢復防護**。

防護狀態

卡巴斯基病毒掃瞄元件的效能都會記錄於報告。報告中您可以檢視已偵測的受感染的檔案及危險檔案數量，並可得知這些檔案是否已經被解毒、刪除或隔離。防護狀態圖示將會以顏色來提醒使用者。當偵測到惡意檔案，狀態圖示將會顯示為紅色，並會建議使用者立刻刪除。

檢視防護狀態資訊：

1. 開啟主控台。
2. 點選**報告**。

排除防護狀態中的問題：

1. 開啟主控台。
2. 點選**報告**。
3. 點選**狀態**頁籤。如果要重新顯示隱藏訊息，請點選**顯示隱藏訊息**。

如何排除已偵測威脅：

1. 開啟主控台。
2. 點選**報告**。
3. 點選**已偵測威脅**頁籤。
4. 按滑鼠右鍵選擇要執行動作的物件，並從選項中選擇執行動作。

檢視防護狀態報告：

1. 開啟主控台。
2. 點選**報告**。
3. 點選**報告**頁籤。若想檢視每項防護更詳細的資訊，請點選**詳細報告**。

安全管理

在應用程式的主控台上，會隨著防護狀態而顯示不同的顏色(紅、黃、綠)。當問題發生時，我們建議立即修正這些問題。

只要按下**立即修復!**，您就可以檢視問題清單，裡面有詳細的說明和解決方案，其先後順序是依照嚴重性來決定：最前面一最嚴重的問題，會顯示紅色狀態圖示；次之一較不重要，會顯示黃色狀態圖示；最後則是一般訊息。

每個問題都有詳細的說明及解決方式：

- **立即清除**：透過對應的按鍵（立即處理、啟用防護)，您可以修正該問題。
- **稍後清除**：假如因為某些原因無法立即清除，您可以稍後再執行這個動作，請點選隱藏訊息。若要再次顯示隱藏訊息，請點選**顯示隱藏訊息**。

注意：若是重大問題即無此選項，例如惡意物件無法解毒、元件損毀或應用程式損壞。

各項防護元件及功能運作

檔案防護

檔案防護可以預防電腦中的檔案受到感染。當系統啟動時檔案防護將會掃瞄您開啟、儲存或執行的檔案。

預設檔案防護將只掃瞄新增及變更的檔案。您可以在安全防護等級調整防護設定。當偵測到威脅時，將會執行所設定的動作，預設是由防護自動選擇動作。

卡巴斯基實驗室專家建議，請不要任意變更防護設定。我們已經最佳化預設的防護設定。如果您變更設定後想要恢復預設值，請點選**預設等級**按鈕。

變更設定方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**檔案防護**。
3. 點選**設定**。
4. 依需求變更設定值。

元件運作演算法

檔案防護在系統啟動時就會啟用，並在記憶體中執行，可用以掃瞄所有開啟、儲存或執行的檔案。檔案防護預設將只掃瞄新增及變更的檔案。

檔案防護演算法運作如下所示：

1. 攔截所有使用者或程式企圖存取的任何檔案。
2. 根據 iChecker 和 iSwift 資料庫分析所截獲檔案的資訊，並判斷是否進行掃瞄。

掃瞄進行時將會執行的動作：

- 根據惡意程式資料庫掃瞄檔案是否感染病毒。資料庫具有所有惡意程式跟已知威脅的描述說明，並提供解毒方法。
- 檔案分析完畢之後，您可以執行的動作為：
  - 如果發現檔案受到感染，檔案防護將會先封鎖該檔案及建立備份，接著進行解毒。如果解毒成功檔案即可恢復使用。解毒失敗則檔案將被刪除。

- 如果檔案偵測出可疑物件，但不確定是否真為惡意程式，檔案防護將會在進行解毒後，將檔案移動至隔離區。
- 如果未於檔案中發現惡意程式，檔案會立刻恢復使用。

檔案防護在檔案受感染或可能受感染時都會以訊息通知，並要求您在詢問視窗中選擇更進一步的動作：

- 隔離檔案。掃瞄完畢後隔離，更新完畢後用新的資料庫再掃瞄一遍。
- 刪除檔案。
- 略過。如果您確定該檔案不包含惡意程式。

郵件防護

郵件防護可以掃瞄經由傳送及接收郵件中的可疑檔案。當系統啟動時，郵件防護將會掃瞄所有藉由 POP3、SMTP、IMAP、MAPI 及 NNTP 傳輸協定傳遞的電子郵件。

您可以在安全防護等級調整防護設定。當偵測到威脅時，將會執行所設定的動作，預設是由防護自動選擇動作。

卡巴斯基實驗室專家建議，請不要任意變更防護設定。我們已經最佳化預設的防護設定。如果您變更設定後想要恢復預設值，請點選**預設等級**按鈕。

變更設定方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**郵件防護**。
3. 點選**設定**。
4. 依需求變更設定值。

元件運作演算法

本元件執行時會在工作列的圖示上顯示掃瞄郵件的圖案。郵件防護演算法運作如下所示：

1. 攔截每一封使用者傳送或接收的郵件。
2. 將郵件分為郵件主旨標題、本文內容及檔案附件進行掃瞄。
3. 郵件的本文內容及檔案附件會經過病毒資料庫及啟發式分析掃瞄是否含有惡意程式。資料庫具有所有惡意程式和已知威脅的描述說明並提供解毒方式，而啟發式分析可以偵測尚未加入資料庫中的新型威脅。
4. 病毒掃瞄完畢之後您可以執行的動作為：
   - 如果郵件的本文內容及檔案附件發現惡意程式，郵件防護將會封鎖郵件並建立備份，接著進行解毒。如果解毒成功，檔案即可恢復存取。若解毒失敗，則郵件或受感染的部分將被刪除。掃瞄處理完畢後，將會於郵件主旨顯示關於處理方式的文字標籤。
   - 如果郵件的本文內容及檔案附件偵測出可疑物件，但不確定是否真為惡意軟體，郵件防護會將可疑檔案移動至隔離區。
   - 如果未於郵件中發現惡意程式，郵件會立刻恢復使用。

- 在 Microsoft Office Outlook，本元件提供可用來微調郵件防護各項設定的外掛模組功能。

- 如果您使用 The Bat!外掛程式，郵件流量規則跟相關應用程序設定將會由 The Bat!控制並忽略原始設定。
- 當使用其他的收信軟體，例如 Microsoft Outlook Express/Windows Mail、Mozilla Thunderbird、Eudora 及 IncrediMail 時，郵件防護將仍會掃瞄藉由 SMTP、POP3、IMAP 及 NNTP 傳輸協定所傳送的郵件。

請注意，當使用Thunderbird郵件用戶端軟體時，如果使用過濾功能從收件匣移動郵件，將不會掃瞄經由IMAP傳輸協定所傳送的郵件。

網頁防護

當您在瀏覽網路時，可能將電腦上所存放的資料暴露在感染惡意軟體的風險中。因為當您下載免費軟體或瀏覽網站時，都有可能遭遇網路攻擊，並使電腦遭到惡意程式滲透。此外，網路蠕蟲也可能在您開啟網頁或下載檔案之前，藉由您的網路連線侵入您的電腦。

網頁防護功能的設計概念就是要確保使用網路時的安全性。本功能可防止資料藉由 HTTP 傳輸協定進入到您的電腦，同時也能防止惡意的指令碼被執行。

網頁防護將會監控 HTTP 流量是否使用受保護的連接埠來通行。最常被用來傳遞郵件及 HTTP 流量的連接埠已經先被列入保護清單。假如您使用未列入清單的連接埠時，您必須先將連接埠加入防護清單，以免遭到封鎖。

如果您經常使用網路，建議您務必使用網頁防護。假如您已經擁有防火牆或其他流量過濾設備，網頁防護也能提供您更多一層的保障。

您可以在安全防護等級調整防護設定。當偵測到威脅時，將會執行所設定的動作，預設是由防護自動選擇動作。

卡巴斯基實驗室專家建議，請不要任意變更防護設定。我們已經最佳化預設的防護設定。如果您變更設定後想要恢復預設值，請點選**預設等級**按鈕。

變更設定方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**網頁防護**。
3. 點選**設定**。
4. 依需求變更設定值。

元件運作演算法

網頁防護演算法運作如下所示：

1. 網頁防護使用威脅資料庫和啟發式分析，用來攔截並分析使用 HTTP 協定開啟的網站或檔案是否含有惡意程式。資料庫具有所有惡意程式跟已知威脅的說明並提供解毒方法，而啟發式分析可以偵測尚未加入資料庫中的新型威脅。
2. 檔案分析完畢之後您可以執行的動作為：
   - 當使用者開啟的網站或檔案含有惡意程式，將會直接遭到封鎖並顯示網站或檔案遭到感染的通知。
   - 如果網站或檔案不包含威脅，將會立刻恢復使用。

指令碼掃瞄演算法如下所示：

1. 網頁防護攔截網頁上的指令碼，掃瞄是否含有惡意程式。
2. 如果偵測到惡意程式，將會立刻封鎖並以彈跳視窗通知使用者。
3. 如果沒有發現惡意程式或威脅，將會立刻恢復使用。

當使用Internet Explorer開啟網頁時才會進行攔截指令碼。

卡巴斯基網址顧問

網頁防護包括卡巴斯基網址顧問，可用來檢查所有網頁中的網址是否存在於可疑網站或釣魚網站資料庫中。您可以建立信任網址清單或需要被掃瞄的網址檢查清單。本模組支援Microsoft Internet Explorer及Mozilla Firefox瀏覽器。

您可以加以設定信任網址清單及網址檢查清單，或是關閉卡巴斯基網址顧問功能。卡巴斯基網址顧問不僅可以由主控台中設定，也能由瀏覽器工具列的圖示中開啟設定視窗。

建立信任網址清單的方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**網頁防護**。
3. 在視窗右方選取**設定**。
4. 於**安全瀏覽**頁籤的**卡巴斯基網址顧問**，點選**掃瞄信任網址外的全部網址**的**排除**。
5. 於**信任網址清單**視窗中點選**新增**加入不掃瞄內容的網址。

建立網址檢查清單的方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**網頁防護**。
3. 在視窗右方選取**設定**。
4. 於**安全瀏覽**頁籤的**卡巴斯基網址顧問**，點選**掃瞄特定網址**的**選擇**。
5. 於**網址檢查清單**視窗中點選**新增**加入要掃瞄內容的網址。

如果您不想使用卡巴斯基網址顧問，設定方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**網頁防護**。
3. 在視窗右方選取**設定**。
4. 於**安全瀏覽**頁籤的**卡巴斯基網址顧問**，取消勾選**檢查網址**。

要開啟瀏覽器上的卡巴斯基網址顧問，請您點選瀏覽器工具列中的卡巴斯基圖示。

封鎖惡意網站

您可以使用卡巴斯基網址顧問來封鎖已知的可疑網站或網路釣魚網站。如果無法確認網站安全性，建議您使用沙盒防護來開啟網站（限IE與Firefox瀏覽器）。使用沙盒防護開啟網站，可以確保您的電腦不會遭受威脅。

封鎖惡意網站的方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**網頁防護**。
3. 在視窗右方選取**設定**。
4. 於**安全瀏覽**頁籤的**封鎖惡意網站，**勾選**封鎖已知惡意網站**。

區域篩選

區域篩選功能將依據您選擇的區域（國家），執行封鎖或允許存取網站的篩選動作，避免連線到屬於高感染率區域（國家）的網站。

開啟區域篩選的設定如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**網頁防護**。
3. 在視窗右方選取**設定**。
4. 於**區域篩選**頁籤，勾選**依網域名稱篩選**，並在下方選單中設定要封鎖、允許存取或提示訊息的區域。

預設將會允許開啟位於您目前所在區域的網站。當您存取其他地區的網站時將會出現提示視窗。

信任網址

您可以建立內容完全受信任的網址清單。網路防護將不會掃瞄這些網址內的資料。如此可以有效地避免網頁防護干擾從已知的網站下載檔案。

設定信任網址的方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**網頁防護**。
3. 在視窗右方選取**設定**。
4. 於**信任網址**頁籤，勾選**設定信任網址**，並按新增來加入網址。

如果您要暫時從信任清單中排除某個網址，您只要取消勾選該網址項目即可，不需要額外刪除。

網路銀行

當使用網路銀行服務時，您需要更多的防護避免重要的機密資料遺失導致財務損失。網頁防護使用沙盒防護開啟瀏覽器，不管下載資料或使用網路銀行的服務，都能為您提供更嚴密的把關及防護。

啟用網路銀行的方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**網頁防護**。
3. 在視窗右方選取**設定**。
4. 於**網路銀行**頁籤，勾選**啟用控制**。啟用後將會開啟憑證安裝精靈來掃瞄加密的連線。
5. 點選**新增**，加入要使用網路銀行或處理機密資料的網址。

還原網頁防護預設值

如果不滿意所變更過的設定，您可以還原至卡巴斯基實驗室所制定的預設值，也就是將所有設定恢復至預設等級。

還原網頁防護預設值的方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**網頁防護**。
3. 於**安全防護等級**點選**預設等級**，即可恢復至預設值。

即時通訊防護

舒適的網際網路除了提供方便性之外，即時通訊軟體也逐漸被廣泛使用。即時通訊軟體卻也成為電腦安全性的潛在威脅，包含可疑網址的即時訊息或是入侵者用來進行網路釣魚攻擊的惡意程式，都會使用即時通訊軟體來進行散播。惡意程式藉由通訊軟體所散發的垃圾訊息或釣魚網址，最常被用來竊取使用者的帳號及密碼。

即時通訊防護的設計理念就是要保護使用即時通訊軟體時的安全性。本防護將會防護即時通訊軟體協議所接收的資訊，例如：ICQ、MSN、AIM、Yahoo! Messenger、Jabber、Google Talk 或其他即時通訊軟體。

由於Yahoo! Messenger及Google Talk軟體使用加密通訊協議（SSL），因此如果要使用即時通訊防護來進行掃瞄，必須設定掃瞄加密連線。請於**設定**的**進階設定**選擇**網路**，勾選**掃瞄加密的連線**。

變更設定方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**即時通訊防護**。
3. 點選**設定**。
4. 依需求變更設定值。

元件運作演算法

即時通訊防護會在系統啟動後開始啟用並在記憶體執行，掃瞄所有傳送與接收的訊息。即時通訊防護演算法運作如下所示：

1. 攔截使用者接收或傳送的訊息。
2. 利用資料庫的數據掃瞄分析訊息中是否含有可疑或網路釣魚網址。如果偵測到威脅將會顯示英文封鎖訊息。
3. 如果掃瞄完畢沒有發現任何威脅將會正常顯示。

當使用即時通訊軟體傳送或儲存檔案時，將會由**檔案防護**進行掃瞄。

應用程式控制

基於系統安全的因素，所有的應用程式可以分為三類：

- **信任**：包含由已知供應商所開發或具有數位簽章的應用程式。您可以允許這類型的應用程式在系統上執行。
- **未信任**：含已知威脅的應用程式。此群組內所有應用程式的動作將會被封鎖。
- **限制**：包含由未知開發者所提供或沒有數位簽章的應用程式。這類型的應用程式可能會破壞作業系統。您必須在使用之前仔細評估應用程式的功能，並分析執行後是否會造成系統安全的顧慮。當您尚未決定使用或安裝這類型的應用程式之前，可以合理的限制該程式存取或使用系統資源。

當應用程式執行時，防護功能將會檢查該程式是否有存取權限，並採取規則中訂定的動作。

變更設定方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**應用程式控制**。
3. 點選**應用程式**。
4. 依需求變更設定值。

或用以下方式開啟：

1. 開啟主控台並選擇**我的防護**。
2. 點選右方**系統及應用程式防護**下**應用程式活動**的**設定**。
3. 依需求變更設定值。

元件運作演算法

第一次使用應用程式，本元件演算法運作如下所示：

1. 掃瞄應用程式是否為病毒。
2. 驗證應用程式的數位簽章。確認完畢後將程式加入**信任**的群組。如果沒有驗證通過、簽章毀損或被列於黑名單，將會需要執行下一步的動作。
3. 於系統內搜尋該應用程式之前的執行記錄。如果有過去的記錄，將會依照記錄新增至之前歸類的群組。如果沒有發現記錄，將會需要執行下一步的動作。

4. 傳送應用程式執行檔的資訊到卡巴斯基實驗室伺服器的已知應用程式資料庫進行分析。當資料庫包含相關資訊，應用程式將會被歸類到對應的群組。如果網路未連線，將會需要執行下一步的動作。
5. 藉由啟發式分析計算應用程式威脅度後，分類到**低限制**的群組。如果應用程式威脅度較高，將會通知您來指定分類的群組。

當所有掃瞄動作完成後，將會顯示關於應用程式控制的通知訊息。預設不會顯示將應用程式新增至信任群組的通知。

當應用程式重新執行後，本元件會檢查程式的完整性。如果應用程式內容沒有變動，將會繼續套用上次執行時的規則。如果程式有變動過，本元件將會以上述演算法重新驗證一次。

系統監控

系統監控會收集所有電腦上應用程式的活動資訊，並將這些資訊提供給其他功能元件進行分析。如果開啟儲存活動記錄功能，當電腦產生任何異常時，您可以執行回溯可疑程式動作。主要在當系統監控偵測到可疑程式行為或免疫防護、檔案防護執行掃瞄發現可疑程式時，使用者可選擇是否執行回溯可疑程式動作。

系統監控於偵測到危險活動或可疑程式時，執行Kaspersky Internet Security預設動作。Kaspersky Internet Security防護元件也可以於偵測到可疑行為時向系統監控功能索取應用程式的額外資訊來協助判斷。當Kaspersky Internet Security使用互動式模式，您可以檢視系統監控所收集的事件記錄，於通知視窗中選擇要執行的動作。如果偵測到潛在的可疑程式，也會有通知視窗顯示，請您選擇下一步要執行的動作。

預設將會自動啟用系統監控。建議您不要關閉此功能，避免緊急狀況時無法使用回溯功能，或無法提供應用程式資訊給免疫防護或其他防護元件來判斷程式是否具有威脅性。

關閉系統監控的方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**系統監控**。
3. 於右方視窗取消勾選**啟用系統監控**。

使用可更新的危險活動模式特徵碼(BSS)

危險活動模式（BSS – 行為數據特徵碼）包含用來定義應用程式是否為威脅的活動類型資料庫。如果應用程式所執行的動作符合危險活動特徵碼，Kaspersky Internet Security將會採取預設動作。
Kaspersky Internet Security更新時將會即時更新危險活動特徵碼資料庫。為了更確實執行系統監控功能，掃瞄任何可能含有危險活動的應用程式，預設將使用啟發式分析，根據特徵碼分析所有應用程式，並在偵測時顯示通知視窗，您可以選擇偵測時要執行的動作。

變更偵測到危險活動時的方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**系統監控**。
3. 右方視窗勾選**啟發式分析**的**使用可更新的危險活動模式特徵碼(BSS)**。
4. 於**選擇動作**的下拉式選單選擇指定的動作。

回溯可疑程式動作

當電腦產生異常時您可以使用此功能將可疑程式的動作回溯。要使用此功能，您必須先啟用儲存活動記錄。回溯可疑程式動作只會影響程式所使用的資料，不會影響到作業系統或電腦上所執行的其他程式。

變更回溯可疑程式動作的方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**系統監控**。
3. 於右方視窗**應用程式活動記錄**勾選**儲存活動記錄**。
4. 於**選擇動作**的下拉式選單選擇指定的動作。

駭客防護

Kaspersky Internet Security 包含一個特殊的防護元件—駭客防護，確保區域網路與網際網路的安全。使用兩個不同類型的規則過濾所有的網路活動：應用程式與網路封包規則。

駭客防護分析您電腦的網路設定。如果應用程式在互動模式中執行，當您第一次連線網路時，駭客防護將會跳出提示訊息，請您指定網路的狀態。如果不使用互動模式，駭客防護將以網路類型、位址範圍與其他條件來指定網路類型。基於不同的網路類型，駭客防護將使用多種規則來過濾網路連線。

變更設定方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**駭客防護**。
3. 點選**設定**。
4. 在**過濾規則**與**網路**頁籤中，修改防火牆設定。

免疫防護

免疫防護除了可以偵測已知威脅，也偵測不在資料庫中的未知威脅。免疫防護提供主動防禦技術，在威脅危害系統前即加以處理。相對的，被動防護技術則是以資料庫記錄來分析惡意程式碼。免疫防護藉由程式的行為來判斷是否為新威脅。當應用程式的活動被判定為可疑行為時，將會封鎖該程式的所有活動。

所有的程式都會進行活動分析，包含應用程式控制的**信任**群組。使用者可停用這些應用程式的免疫防護通知。

相對於**應用程式控制**而言，免疫防護立即對定義的應用程式行為做出反應。

變更設定方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**免疫防護**。
3. 點選**設定**。
4. 依需求變更設定值。

網路攻擊防護

網路攻擊防護在作業系統啟動時載入，追蹤網路流量是否含有網路攻擊的特徵。一旦在電腦上偵測到網路攻擊，Kaspersky Internet Security 會對進行攻擊的電腦進行封鎖，預設的封鎖時間為 60 分鐘。通知訊息會出現在螢幕上，並顯示攻擊的相關資訊，此訊息也代表網路攻擊已被阻擋。

Kaspersky Internet Security 資料庫包含目前已知的網路攻擊與封鎖方式。當應用程式資料庫更新時，也會一併更新網路攻擊防護清單。

垃圾郵件防護

Kaspersky Internet Security 包含垃圾郵件防護，該元件偵測不請自來的郵件並依據規則進行處理。

垃圾郵件防護使用*自我訓練演算法*，讓元件從郵件中篩選出垃圾郵件。

演算法的資料來源是電子郵件的內容。為了有效識別垃圾郵件，垃圾郵件需要有效的郵件進行訓練。因此我們強烈建議您詳細檢視垃圾郵件防護的演算法。

垃圾郵件防護的嵌入式元件包含於下列的郵件收發軟體：

- Microsoft Office Outlook
- Microsoft Outlook Express（Windows Mail）
- The Bat！
- Thunderbird

您可以在垃圾郵件防護中使用允許與封鎖的寄件者，來辨視是否為正常或垃圾郵件。除此之外，垃圾郵件防護也可以檢查在允許和封鎖清單中的詞組，與淫褻文字清單。

垃圾郵件防護允許您檢視伺服器上的郵件與刪除垃圾郵件，而不需將郵件下載至電腦中。

變更設定方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**垃圾郵件防護**。
3. 點選**設定**。
4. 依需求變更設定值。

元件所採用的演算法

垃圾郵件防護運作時分為兩個階段：

1. 應用程式對郵件進行嚴格的篩選。這些判斷準則能夠快速辨識該封郵件是否為垃圾郵件或正常郵件。垃圾郵件防護會為郵件指派狀態：*垃圾郵件*或*非垃圾郵件*，然後郵件將停止掃瞄並轉送到用戶端進行處理。
2. 經過前一步驟嚴格篩選的郵件，若這些郵件不能明確的被視為垃圾郵件，垃圾郵件防護會計算這些郵件的垃圾郵件積分。

垃圾郵件防護演算法包含以下步驟：

1. 檢查郵件的寄件者是否位於允許或封鎖的清單中。
   - 若寄件者的位址位於允許清單中，該郵件將歸類於*非垃圾郵件*。
   - 若寄件者的位址位於封鎖清單中，該郵件將歸類於*垃圾郵件*。
2. 如果郵件是透過 Microsoft Exchange Server 寄送，而掃瞄郵件的功能已停用，該郵件將被歸類為*非垃圾郵件*。
3. 透過比對允許詞組清單，分析該郵件。如果在該清單中至少符合一個項目，該郵件將被歸類為*非垃圾郵件*。預設略過此步驟。
4. 除了檢查郵件的內容字串是否包含在封鎖的清單中，也會分析郵件中的字串是否包含在淫穢文字清單中，再根據郵件中的文字訊息來判斷是否提高為垃圾郵件的積分。如果計算出來的積分超過所指定的值，郵件就會被判定為*垃圾郵件*或*可能為垃圾*。預設略過此步驟。
5. 如果郵件中的文字包含在網路釣魚或可疑網站中，該郵件將被判定為*垃圾郵件*。
6. 使用啟發式分析郵件。如果分析結果是典型的垃圾郵件，那該封郵件的垃圾郵件積分就會增加。
7. 應用程式使用 GSG 演算法進行分析。當採取此種演算法時，垃圾郵件防護分析郵件內容中的圖片。如果分析結果是典型的垃圾郵件，那該封郵件的垃圾郵件積分就會增加。
8. 應用程式也可以分析附加在電子郵件中的 *RTF* 格式文件，檢查附件是否為垃圾郵件。在分析完成之後，垃圾郵件防護計算郵件為垃圾郵件的積分。預設停用此技術。
9. 使用額外的功能檢查是否為典型的垃圾郵件。每個偵測功能都會增加垃圾郵件積分。
10. 如果垃圾郵件防護已進行訓練，郵件將使用 iBayes 技術進行掃瞄。自我訓練 iBayes 演算法計算郵件中的詞組為垃圾郵件的機率。

郵件經過分析後，會計算出垃圾郵件積分。垃圾郵件的作者不斷的改良偽裝成正常郵件的方法，因此垃圾郵件積分可能不會達到指定的值。為了確保更有效率的過濾進出的郵件，垃圾郵件防護使用兩種參數：

- **垃圾郵件積分**：當超過設定的數值，該封郵件就會被視為*垃圾郵件*。如果低於此值，該郵件就會被視為*疑似垃圾郵件*。
- **疑似垃圾郵件積分**：當超過設定的數值就會被判定為*疑似垃圾郵件*。如果積分小於此值，垃圾郵件防護就將該郵件視為*非垃圾郵件*。

基於指定的垃圾郵件與疑似垃圾郵件的積分，郵件將被視為**垃圾郵件**或**疑似垃圾郵件**。依其被指派的狀態，在郵件主旨的欄位將被標示為**[!! SPAM]**或**[?? Probable Spam]**，然後依據所設定的規則進行處理。

廣告橫幅防護

廣告橫幅防護封鎖應用程式或瀏覽器中顯示的橫幅。廣告橫幅不僅缺乏有用的資訊，他們還會吸引你的注意，增加電腦的資料傳送量。廣告橫幅防護除了封鎖目前已知種類的橫幅，也會使用包含在 Kaspersky Internet Security 中的遮罩進行篩選。您可以停用廣告橫幅防護或自行建立允許與封鎖的清單進行篩選。

在 Kaspersky Internet Security 安裝程式中，包含卡巴斯基實驗室專家所編輯的廣告橫幅清單。只要有符合清單中所設定的項目，將會由廣告橫幅進行封鎖。不包含在清單中的位址，則可透過啟發式分析進行封鎖。

除此之外，您也可以建立允許與封鎖的清單，決定允許或封鎖該廣告橫幅。

在安裝 Kaspersky Internet Security 之後，廣告橫幅預設停用。

設定廣告橫幅防護：

1. 開啟主控台並點選右上方的**設定**。
2. 於**防護中心**選擇**廣告橫幅防護**。
3. 點選**設定**。
4. 依需求變更設定值。

家長控制

家長控制功能可以限制或監控使用者操作電腦或存取網路。除了提供更彈性的選項來控制存取資源或應用程式外，還有提供報告功能讓您隨時可以瀏覽更完整的資訊。因為網路氾濫的資訊沒有受到管制，近年來幼童或青少年使用電腦或上網時接觸到不良資訊的情形日益嚴重，同時也對電腦產生更多威脅。最常見的狀況如下：
開啟浪費時間（聊天室、遊戲）、金錢（網路商店、拍賣）或含有成人內容（色情、槍械、毒品、挑釁、暴力）的網站；下載含有病毒的程式或檔案；使用電腦的時間過久，導致身心健康受到影響；接觸陌生網友時洩漏了個人隱私身分資訊（真實姓名、地址）。

變更設定方式如下：

1. 開啟主控台並點選右上方的**設定**。
2. 於**進階設定**選擇**家長控制**。
3. 點選**設置**。
4. 依需求變更設定值。

元件運作演算法

使用家長控制功能即可避免發生上述狀況，進而減低遭受威脅的風險。家長控制演算法運作如下所示：

在使用者帳戶登入後，將自動套用相對應的設定。

- 電腦使用：控制電腦的使用頻率及時間。
- 應用程式使用：建立允許或封鎖的應用程式清單，並可控制允許執行的應用程式使用頻率及時間。
- 網路使用：控制網路的使用頻率及時間。
- 網路瀏覽：啟用安全搜尋功能（過濾搜尋引擎的結果，含有可疑內容的網站將不會顯示），並可建立允許或封鎖的網站清單，或是封鎖特定類別的網站。
- 檔案下載：控制可以從網路下載的檔案類別。
- 即時通訊：建立使用即時通訊軟體時，允許或封鎖的聯絡人清單，並檢視傳送內容。
- 社交網路：建立使用社交網路時，允許或封鎖的聯絡人清單並檢視訊息內容。
- 隱私資料：封鎖傳送隱私資料的行為。
- 關鍵字使用：搜尋傳送訊息中的關鍵字使用情形。

所有控制功能都可以個別啟用，讓您方便且彈性地管理不同使用者帳戶設定。您也可以檢視每個帳戶各項功能的操作報告。

開始使用家長控制功能之前，您必須先設定管理者的帳號及密碼完成認證程序。如果您忘記設定密碼，Kaspersky Internet Security 將會提示您完成此動作。

沙盒防護

沙盒防護無法於 *Windows XP* 64 位元系統上執行。而安裝於 *Windows 7* 64 位元、*Windows Vista* 64 位元作業系統時，沙盒防護部分功能會受到限制。

為確保作業系統檔案及使用者個人資料受到最安全的防護，卡巴斯基實驗室研發「**沙盒防護**」功能，此功能可將第三方軟體在受到良好防護的虛擬環境下執行。

建議您洽詢卡巴斯基的技術人員協助使用沙盒防護功能，並請務必不要任意將作業系統或其他軟體的執行程序加入沙盒防護，以避免發生不當的操作行為，或修改系統或軟體，進而造成執行錯誤。

在Windows 7 64位元和Windows Vista 64位元作業系統使用沙盒防護可能會受到一些限制。當此狀況發生時，如果您有設定通知訊息，將會於畫面顯示**應用程序功能受沙盒防護限制**。

於沙盒防護開啟瀏覽器程式，可以保障瀏覽網頁時不會遭受惡意程式的滲透，保護使用者的個人資訊不會未經同意即被刪除或修改。而且，當瀏覽結束時，也可以清除所有衍生的檔案：暫存檔、Cookie 及瀏覽記錄。

您可自行決定是否使用沙盒防護來開啟應用程式。沙盒防護也提供建立捷徑功能，來協助您迅速啟動沙盒防護的應用程式。

當應用程式於沙盒防護執行時，該程式的檔案仍可進行修改或存取。您也可以利用沙盒防護資料夾來存放這些檔案。當清除沙盒防護應用程式中的資料時，存放於沙盒防護資料夾中的檔案仍會保留。

如果您希望透過沙盒防護來執行應用程式，建議您以作業系統的標準模式安裝應用程式。

掃瞄我的電腦

掃瞄系統中的病毒及弱點是確保電腦安全性的重要工作之一。病毒掃瞄將會偵測惡意程式是否蔓延。弱點掃瞄將協助您檢查出系統內可能遭入侵者用來傳播惡意程式或竊取個人資料的漏洞。

卡巴斯基實驗室的專家將掃瞄工作區分為以下類型：

- **自訂掃瞄**：由使用者自行決定掃瞄物件。電腦中的任何物件都能掃瞄。您也可以使用此工作來掃瞄移動式儲存裝置。
- **完整掃瞄**：針對系統內所有物件進行完整的掃瞄，包括系統記憶體、隱藏的啟動檔案、系統備份儲存區、全部的硬碟機，及全部的抽取式硬碟。
- **快速掃瞄**：針對系統記憶體、隱藏的啟動檔案，及磁碟開機磁區進行掃瞄。

建議不要變更完整掃瞄及快速掃瞄的掃瞄範圍檔案清單。

更新

使資料庫定期更新是防護電腦的必要條件。每天都會產生新的病毒、木馬程式或惡意程式，因此隨時更新資料庫來保障電腦安全顯得非常重要。關於威脅的資訊及解決方法都存放於卡巴斯基實驗室的資料庫中，定期下載這些資料檔案就能維持最佳的防護效果。

更新資料庫將會下載檔案到您的電腦中：

- **卡巴斯基資料庫**：包含惡意威脅、網路攻擊特徵碼及解決方法的防護資訊。各項防護元件將依此資料庫來偵測及解毒。由於卡巴斯基實驗室資料庫每小時發佈威脅資訊，建議您務必定期更新資料庫。
- **應用程式模組**：除了更新資料庫外，還會下載含有卡巴斯基弱點的更新修正套件，下載安裝完畢即可修復既有的弱點或加強功能與運作效率。

為了由卡巴斯基伺服器完整下載更新，您必須先確認網路可正常連線。預設的更新方式是藉由網際網路連線至伺服器下載，若您是採用代理伺服器連線，請手動設定相關資訊。

更新成功後會在更新中心顯示資料庫狀態為最新。當您的資料庫過舊時，將會出現提示訊息，請您馬上進行更新。如果太久沒有更新，所需要下載的資料庫檔案量可能會較大，請您耐心等候下載完成。每一次的更新資料將會自行備份，萬一更新失敗或資料庫毀損時可以隨時**回溯至前一版的資料庫**。

安全工具箱

確保系統安全不是一項簡單的工作，需要熟悉作業系統特性及系統漏洞的專家協助。此外，系統資源的數量及多變性也會增加分析和處理的難度。

為了協助能更具體減低各項的安全性疑慮，卡巴斯基實驗室推出了一系列能加強系統防護的精靈及工具：

- **救援光碟建立精靈**：如果遭受病毒危害後或系統檔案毀損造成無法開機時，仍可恢復系統運作。
- **弱點掃瞄**：精靈會進行系統的安全診斷以及檢查程序中那些具有潛在的漏洞，並產生一份需要執行的動作清單來修復系統漏洞。
- **瀏覽器設定精靈**：針對 Microsoft Internet Explorer 瀏覽器的安全性進行診斷評估。
- **隱私清理精靈**：搜尋並清除各種的使用者活動記錄。
- **系統還原精靈**：搜尋並清除惡意軟體活動的相關問題。

報告

Kaspersky Internet Security 會建立每個防護功能的執行報告。藉由報告您可以檢視相關資訊。例如指定時間內已偵測或已刪除的可疑程式（病毒檔案或木馬程式）、更新歷程及更新檔案資訊、已偵測的垃圾郵件訊息或其他功能詳細執行資訊。

當您使用 Microsoft Windows Vista 或 Microsoft Windows 7 作業系統時，您可以利用卡巴斯基小工具來開啟報告。卡巴斯基小工具左邊圖示預設為開啟報告，您可以於設定選項中設定左右邊圖示要開啟的功能。

開啟報告的方式如下：

1. 開啟主控台並點選右上方的報告，或使用卡巴斯基小工具上的圖示開啟（Microsoft Windows Vista 或 Microsoft Windows 7 作業系統）。
   報告頁籤會以圖表方式顯示已掃瞄偵測的相關資訊。

2. 如果您要檢視每項防護功能更詳細的資訊，請點選報告頁籤右下方的**詳細報告**。

   詳細報告視窗將會以日期來區分相關資訊。要更快速檢視內容，您可以輸入關鍵字來搜尋指定資訊。

通知訊息

當卡巴斯基執行事件時將會有相對應的通知訊息顯示。根據事件的嚴重性，您會接收到下列三類的通知訊息：

- **嚴重**：重大事件通知，例如在系統上發現惡意物件的危險動作。您必須立即決定如何處理威脅。這類型的通知為紅色提示視窗。
- **警告**：具有潛在威脅的事件通知。例如在系統上發現可能被感染的檔案或可疑活動行為。您可以根據提示訊息判斷類似的檔案或行為是否具危險性。這類型的通知為黃色提示視窗。
- **資訊**：此類通知提供非重大事件的資訊。這類型的通知為綠色提示視窗。

通知訊息視窗包含四個部分：

- **視窗標題**：包括簡短的事件描述，例如：可疑的活動行為、提示執行權限、偵測到新的網路連線或病毒警告等。
- **事件描述**：顯示關於訊息的詳細資訊，例如：某個應用程式名稱所引起的事件、偵測到的威脅名稱或已偵測的網路連線設定。
- **選擇動作**：卡巴斯基將會於訊息中顯示建議的動作。根據事件類型會有相關的建議選項，例如偵測到病毒時：**解毒**、**刪除**或**略過**。應用程式是否能夠執行，以免對系統造成危害：**允許**及**封鎖**。由卡巴斯基實驗室專家建議的選項將會以粗體字註明。
- **進階動作**：**新增至排除清單**。如果您確定檔案或程序不具威脅性，建議您可以將它加入信任區域，避免下次您使用時重複提示。**套用至所有檔案**，將所做的設定或動作直接套用至其他相同的事件。

疑難排解

如果您在使用上發生問題時，首先可以到我們的官方網站尋找問題解答：
http://web.kaspersky.com.tw/KL-Services/FAQ.htm

點選「個人用戶」後依照您的軟體版本進行選擇，再依據所發生的問題種類尋找相關技術支援文章。每篇文章內都有卡巴斯基實驗室專家建議的操作方式，協助您排除問題。

如果您在常見問題解答找不到適當解決方法，請連絡技術支援中心：
http://www.kaspersky.com.tw/KL-Services/techsupport.htm